

**PATENT APPLICATION**

**METHODS AND SYSTEMS FOR UNIVERSAL TRANSACTION  
PROCESSING**

Inventor(s): Steven L. VanFleet, a citizen of the United States, residing at  
160 Range Road  
Southport, CT 06890

John J. Mascavage III, a citizen of the United States, residing at  
701 Harvard Road  
San Mateo, CA 94402

Matthew T. Byrne, a citizen of the United States, residing at  
906 Killarney Drive  
Papillion, NE 68046

Diane Wing, a citizen of the United States, residing at  
1024 Huntington Road  
East Lansing, MI 48823-4126

Cassandra J. Mollett, a citizen of the United States, residing at  
8426 East Shetland Trail  
Scottsdale, AZ 85258

Assignee: First Data Corporation  
12500 East Belford Avenue  
Englewood, CO 80112

Entity: Large

## **METHODS AND SYSTEMS FOR UNIVERSAL TRANSACTION PROCESSING**

### 5                                   CROSS-REFERENCES TO RELATED APPLICATIONS

[0001]           This application is related to the following co-pending, commonly-assigned and concurrently filed U.S. Patent Applications, the entirety of each of which are herein incorporated by reference for all purposes: U.S. Patent Application No. --/---,---, entitled  
10   “METHODS AND SYSTEMS FOR ONLINE TRANSACTION PROCESSING” (Attorney Docket No. 020375-050000); and U.S. Patent Application No. --/---,---, entitled “METHODS AND SYSTEMS FOR PRIVATE LABEL TRANSACTION PROCESSING” (Attorney Docket No. 040143-050200).

### 15                                   BACKGROUND OF THE INVENTION

[0002]           This application relates generally to transaction processing. More specifically, this application relates to methods and systems for debit transaction processing.

[0003]           Consumers may pay merchants for purchases using a variety of payment  
20   types. Typically, these payment types include cash, checks, and credit cards. Consumers may also elect to pay for purchases using a debit card. Debit cards are typically issued by the financial institution at which the consumer maintains a financial account and are used to debit the financial account for purchases or other services.

[0004]           There are generally two types of debit cards. The first type of debit card is  
25   processed by an association, such as MASTERCARD. To the merchant, these types of cards are processed similar to a credit card, with similar high transaction costs incurred by the merchant. A second type of debit card may use a debit-based system to process the transaction. These debit cards are usually the same cards that a consumer may use to access an Automated Teller Machine (ATM). Typically, the consumer is required to enter a  
30   Personal Identification Number (PIN) at the time of the transaction to use the card. The second type of debit card usually results in a lower transaction cost to the merchant, but not all merchants accept these cards. Additionally, while lower than a credit-based transaction,

the transaction costs are still higher than other networks, such as an automated clearing house (ACH) network used to transfer funds between financial institutions.

## BRIEF SUMMARY OF THE INVENTION

**[0005]** Methods and systems are disclosed for universal debit transaction processing.

In one embodiment, a method is disclosed which comprises receiving, at a payment network,

5 a first information packet from a merchant. The first information packet includes a cost of a financial transaction between the merchant and a customer. The first information packet also includes a credential presented by the customer as payment for the financial transaction. The payment network uses the credential to determine account information that identifies a financial account maintained by the customer at a financial institution and authorization  
10 information that allows debit access to the identified financial account. The payment network then generates a second information packet comprising the account information and the authorization information. The payment network selects one of a plurality of transaction networks over which to transmit the second information packet to the financial institution. The second information packet is then transmitted from the payment network to the financial  
15 institution using the selected transaction network, with a request to perform a debit transaction from the identified financial account for at least a portion of the cost of the financial transaction.

**[0006]** In some embodiments, the method may additionally comprise using the

credential to determine, with the payment network, second account information and second  
20 authorization information. The second account information identifies a second financial account maintained by the customer at either the financial institution or a second financial institution, and the second authorization information is information that allows debit access to the identified second financial account. The payment network may also determine an apportionment of the cost among the first and second financial accounts and may generate a  
25 third information packet comprising the second account information, the second authorization information, and a portion of the cost to apply to the second financial account in accordance with the apportionment.

**[0007]** The method may also comprise receiving, at the payment network, a response from the financial institution. The response indicates approval or denial of the debit

30 transaction. The payment network then transmit an authorization code to the merchant indicating approval or denial of the financial transaction in accordance with the response received from the financial institution. The payment network may also perform a risk analysis of the financial transaction and determine whether to provide a guarantee of the

transaction to the merchant based on the risk analysis. The authorization code could also reflect whether the guarantee is provided.

**[0008]** Transmission of the second information packet to the financial institution may be accomplished in different ways. In one embodiment, the second information packet may be transmitted to the financial institution over an automated clearing house ("ACH") network. In another embodiment, the second information packet may be transmitted to the financial institution over a debit system. In a third embodiment, the second information packet may be transmitted directly to the financial institution. The transaction network may be selected based on a risk analysis performed on the financial transaction.

**[0009]** The information comprised by the first information packet may vary according to the embodiment. For instance, in one embodiment, the credential may comprise a payment network account number assigned to the customer to access the payment network. In some embodiments, the credential may further comprise a personal identification number (PIN) and the method may additionally comprise verifying the PIN is associated with the payment network account. Additionally, in some embodiments, the financial transaction may be for an Internet-based financial transaction.

**[0010]** In a second embodiment, a method is disclosed which comprises receiving, at a payment network, an information packet from a merchant. The information packet includes a cost of a financial transaction between the merchant and a customer and a credential assigned to the customer. The credential is used to determine account information for a plurality of accounts identifying a plurality of financial accounts maintained by the customer at one or more financial institutions. The payment network uses the credential to determine authorization information for each of the identified financial accounts that allows access to the identified financial account. The payment network also determines an apportionment of the cost to apply to each of the identified financial accounts. The payment network then generates a plurality of authentication packets for each of the identified financial accounts. Each authentication packet comprises account information for one of the identified financial accounts, authorization information for the identified financial account, and the determined apportionment of the cost to apply to the identified financial account. The payment network transmits each of the authentication packets to the respective financial institution at which the financial account is maintained.

[0011] In one embodiment, a response may be received at the payment network indicating denial of the debit transaction. The payment network may then transmit an additional authentication packet including account information for a second one of the identified financial accounts different from the financial account associated with the denied authentication packet. The additional authentication packet also includes authorization information for the second financial account and the determined apportionment of the cost comprised by the denied authentication packet. Alternately, in a different embodiment, if a response is received at the payment network indicating denial of any of the authentication packets, an authorization code may be sent to the merchant indicating denial of the financial transaction. If all responses to the authentication packets indicate approval of the debit transaction, the authorization code may be sent to the merchant indicating approval of the financial transaction.

[0012] The apportionment of the cost to apply to each of the identified financial accounts may be performed in a variety of ways. For instance, the cost may be apportioned equally among the identified financial accounts. As a second example, the costs may be allocated using an allocation apportionment specified by the customer.

[0013] In a third embodiment, the method may comprise receiving, at a payment network, account information that identifies a plurality of financial accounts maintained by a customer at one or more financial institutions and authorization information for each of the identified financial accounts that allows debit access to the respective identified financial account. The payment network then verifies the account information and authorization information for each of the identified financial accounts. A credential is associated to the customer account information and the authorization information. The payment network transmits an enrollment approval for the customer.

[0014] The methods may be embodied in a payment network having a communications device, a processor, a storage device, and a memory coupled with the processor. The memory comprises a computer-readable medium having a computer-readable program embodied therein for directing operation of the payment network. The computer-readable program includes instructions for operating the computer system to manage information in accordance with the embodiments described above.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Illustrative embodiments in accordance with the invention are illustrated in the drawings in which:

5 [0016] Fig. 1 is a block diagram of a system that may be used for universal debit transaction processing;

[0017] Fig. 2 is a block diagram illustrating a payment network that may be used in the system of Fig. 1;

10 [0018] Fig. 3 is a block diagram of a computer system on which methods of the invention may be embodied;

[0019] Fig. 4 is a flow diagram illustrating an exemplary method for enrolling a customer into the payment network; and

[0020] Fig. 5 is a flow diagram illustrating an exemplary method for performing universal debit transaction processing.

15

## DETAILED DESCRIPTION OF THE INVENTION

[0021] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

20 [0022] Methods and systems are provided for universal debit transaction processing. The debit transactions may be used to pay for a financial transaction between a merchant and a consumer. The financial transaction may involve the purchase of goods and/or services from the merchant. An overview of one system that may be used to support universal debit transaction processing is illustrated in Fig. 1.

25 [0023] The system includes a payment network 100, which may be interfaced to different types of systems that may be used in supporting debit transactions. For example, one such system is the automated clearing house ("ACH") system 120, which is an electronic

30

payment-delivery system known to those of skill in the art. The ACH system comprises a network that provides batch-oriented electronic funds transfer governed by the NACHA operating rules. Briefly, the ACH network provides ACH operators that act as an interface between originating and receiving depository financial institutions. Transactions received at a financial institution 140 during a day may be stored and processed later in batch mode to exploit economies of scale. Debit transactions may also be supported by a debit system 130, sometimes referred to in the art as a network that comprises “debit rails” for effecting communications between financial institutions 140 to execute debit transactions from demand deposit accounts (“DDAs”). The interconnection provided by such debit rails of the debit system 130 allows real-time access to a customer’s DDA information, including account balance, so that real-time debits of the DDA may be made. For example, such debit rails may be provided by known networks such as the NYCE<sup>®</sup> network, the Pulse<sup>®</sup> network, the STAR<sup>®</sup> network, and the like. In still other instances, an intermediary system like the ACH system 120 or debit system 130 may be avoided by using a direct connection to a financial institution 140, providing so-called “direct-to-bank” interactions.

**[0024]** The payment network 100 may be directly connected to merchant 110 so that transaction information entered into between merchant 110 and customers may be communicated to the payment network 100 to support the transaction. By way of example, point-of-sale devices (not shown) at the merchant location may be communicatively coupled to the payment network 100. In alternate embodiments, merchant 110 may connect to the payment network through the Internet or other communication means. It should be appreciated that more than one merchant 110 location may be communicatively coupled to the payment network 100. Additional merchants 110 and financial institutions 140 may also be communicatively coupled to the payment network 100.

**[0025]** The security of information communicated between the payment network 100 and merchant 110 is generally greater with a direct connection. This is reflected by the illustration of Fig. 1 in which the payment network 100 is provided with interconnections to the ACH system 120, debit system 130, and direct links to financial institutions 140. As will be described in further detail below, the most sensitive financial information during transactions is communicated on this side of the system.

**[0026]** Parties may register with the payment network 100 using a registrar 150. Registrar 150 may be a separate entity as shown in Fig. 1 or may be merchant 110 or

financial institution 140. In some embodiments, customers may be able directly register with the payment network 100.

**[0027]** Details of the payment network 100 may be understood more fully with reference to Fig. 2, which shows an exemplary embodiment of the payment network 100.

5 The payment network 100 may comprise a transaction gateway 208 and a transaction system 220, both of which may comprise a plurality of modules used in supporting transactions. The transaction gateway 208 may include an authentication module 212 that authenticates information provided by a merchant 110 during a transaction. The authentication module 212 interacts with an authorization module 224 of the transaction system 220 to coordinate  
10 seeking an authorization for the transaction. In addition, the transaction gateway 208 may further include a clearing/settlement module 216 that interacts with a clearing module 228 and a settlement module 232 of the transaction system 220 to perform clearing and settlement functions.

**[0028]** The transaction system 220 may also include an enrollment module 236 to  
15 accommodate different methods of enrollment. By way of example, customers may be enrolled by registrar 150, financial institution 140, or merchant 110. Customers may also request enrollment themselves by interacting directly with enrollment module 236 (e.g., using an Internet-based or other type of interface). The enrollment module 236 may also be in communication with a card-embossment facility 240 to accommodate those embodiments in  
20 which enrollment of a customer may be coupled with preparation of a magnetic-stripe or other type of card.

**[0029]** The structure shown in Fig. 2 emphasizes certain aspects of the arrangement that illustrate its flexibility and integration into existing financial infrastructures. For instance, in any given transaction between a merchant 110 and a customer, the customer may  
25 still have the option of executing the transaction with different mechanisms. Thus, while the solid lines between the merchants 110 and the transaction gateway 208 indicate paths that may be followed if the customer elects to perform a debit transaction using a credential assigned to the customer to access the payment network, the dashed lines indicate pathways to a credit-card network 204 that may be used if the customer elects to perform a credit  
30 transaction. The infrastructure illustrated in Fig. 2 may thus be integrated with existing infrastructures without compromising the performance of such existing infrastructures. The interconnection of the payment network 100 with existing ACH systems 120, debit systems

130, or financial institutions 140 are coordinated with the transaction system 220 in the illustrated embodiment, but may be coordinated by the transaction gateway 208 in certain other embodiments.

[0030] It should be appreciated that alternate embodiments of payment network 100 may not include all the components illustrated in FIG. 2 or may include different components. For instance, the functionality provided by transaction gateway 208 and transaction system 220 may be combined into one component. As another example, the modules of transaction gateway 208 and/or transaction system 220 may be combined or may be further separated into additional modules.

[0031] While Fig. 2 illustrates a logical structure for the payment system 100, Fig. 3 provides a schematic illustration of a physical structure that may be used to implement the transaction gateway 208 and/or transaction system 220 in one embodiment. Fig. 3 broadly illustrates how individual system elements may be implemented in a separated or more integrated manner. The structure 208/220 is shown comprised of hardware elements that are electrically coupled via bus 326, including a processor 302, an input device 304, an output device 306, a storage device 308, a computer-readable storage media reader 310a, a communications system 314, a processing acceleration unit 316 such as a DSP or special-purpose processor, and a memory 318. The computer-readable storage media reader 310a is further connected to a computer-readable storage medium 310b, the combination comprehensively representing remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing computer-readable information. The communications system 314 may comprise a wired, wireless, modem, and/or other type of interfacing connection and permits data to be exchanged with the merchants 110, between the transaction gateway 208 and transaction system 220, with the ACH system 120, with the debit system 130, with the financial institution 140, with the card-embossment facility 240, or with any other external system as may be desired in implementing embodiments as described below.

[0032] The structure 208/220 also comprises software elements, shown as being currently located within working memory 320, including an operating system 324 and other code 322, such as a program designed to implement methods of the invention. It will be apparent to those skilled in the art that substantial variations may be made in accordance with specific requirements. For example, customized hardware might also be used and/or

particular elements might be implemented in hardware, software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[0033] The architecture described above may be used in a variety of embodiments to implement debit-based transactions. Use of the architecture may include enrollment functions, in which customers are assigned a private label card account number and/or credentials that may be used as a mechanism for identifying the customer and the account to be used in the private label card debit transactions. The private label card account number may be embossed on a magnetic-stripe card. The customer may additionally be assigned additional identifying credentials, such as a personal identification number ("PIN"). For security, the PIN may be assigned to the customer separately. Other credentials are also envisioned. Once the customer has been assigned a private label card account number and has enrolled in the payment network 100, he or she may engage in debit-based transactions using the private label card. As executed transactions accumulate, there may be periodic clearing and settlement functions performed to reconcile the transactions.

[0034] Fig. 4 is a flow diagram that illustrates an exemplary embodiment for enrolling a customer into the payment network 100. Enrollment module 236 receives information identifying one or more customer accounts, such as demand deposit accounts ("DDAs") from which funds are to be debited when the customer uses the private label card enrolled in the payment network 100. Such identification is typically made by the customer providing the primary account number ("PAN") for the identified financial account(s) along with suitable financial-network routing information. The enrollment module 236 also receives authorization information that allows debit access to the identified financial account(s). For example, the authorization information may comprise a personal identification number ("PIN") assigned to the customer for accessing the identified financial account. In instances where more than one account is identified, a profile may be received or setup by the enrollment module 236 to identify allocations of debit transactions among the multiple accounts or specific identifications may be made at the time of a transaction.

[0035] The customer account information and authorization information may be provided to enrollment module 236 in a variety of different ways. In one embodiment, the information may be provided by a registrar 150 entering the information into a direct interface to enrollment module 236 or using an internet enrollment 244 interface. In another

embodiment, the information may be received 402 from the financial institution 140 or merchant 110 using a direct interface to the enrollment module 236 or the internet enrollment 244 interface. In some embodiments, the customer may also enroll in the payment network directly using internet enrollment 244 interface. It should be appreciated that alternate  
5 interfaces may also be used to enroll the customer into the payment network 100.

**[0036]** Once the enrollment module 236 has collected the identification information, a verification 406 may be performed. Such verification may involve communications with the financial institution that maintains the identified account(s) to confirm the authenticity of the account information and authorization information (existence of the account, its ownership by  
10 the customer, correct authorization information, etc.). In some instances, the verification at block 406 may additionally include a risk-analysis based on such factors as the balance maintained in the identified account, credit score of the customer, demographic information regarding the customer, and the like. Approval of the customer to participate with the payment network 100 may depend in such instances not only on verification of the account  
15 status, but also on the customer having a satisfactory risk level.

**[0037]** If the customer information is accepted, the enrollment module 236 generates 408 a credential to be assigned to the customer to access the payment network 100. The credential may include an account number for the payment network. In some embodiments, the credential may also include a PIN associated with the payment network account number  
20 to provide additional security. In alternate embodiments, the credential or a portion of the credential (e.g., either or both of an account number and a PIN) may be provided to the enrollment module 236.

**[0038]** As described above, in some embodiments, the customer may provide more than one financial account from which funds are to be debited for future financial transactions entered into by the customer. In these embodiments, the enrollment module 236 may also be  
25 provided with an allocation apportionment for each of the financial accounts indicating the portion of future financial transactions to allocate to each of the identified financial accounts. Other types of instructions for allocating costs of future financial transactions may additionally or alternately be received. By way of example, accounts may be prioritized, and  
30 lower priority accounts may only be used if higher priority accounts are denied or otherwise unavailable for use.

**[0039]** The enrollment module associates 410 the credential with the account(s) specified during enrollment. Additional information, such as instructions on how future financial transactions are to be allocated between accounts, may also be associated with the credential. The association of the credential with the account(s) specified by the user allows the payment network 100 to convert the credential to a form of information suitable for performing a debit transaction when the credential is used to pay for later financial transactions between the customer and the merchant 110. For example, the credential may be used to determine one or more PAN/PIN combinations used to ride the debit rails 130 or may be used to generate information suitable for one or more ACH transactions or one or more direct-to-bank transaction. The mapping between credentials and conventional debit-transaction identification information is maintained securely by the transaction gateway 208. Since this conventional information is not transmitted during transaction processing, there is little risk of it being compromised. In the event that the credential assigned to the customer is stolen, a different credential may be substituted without needing to change account information at the financial institutions where the account(s) are held.

**[0040]** Assuming the enrollment process was completed successfully, an enrollment approval may then be transmitted 412 to the user (e.g., registrar, customer, etc.) requesting enrollment. Additional information may also be transmitted to the user, such as credentials assigned to the customer. Some information may alternately or additionally be sent to the customer at a later time. For instance, a letter with a PIN number assigned to the customer may be mailed separately. The enrollment module 236 may also initiate a request to a card embossment facility 240 to generate 414 a new card magnetically encoded with the payment network account number (or other credential information). It should be appreciated that in some embodiments merchants may also need to be enrolled into the system in order to have the ability to accept the customer's credentials as payment for transactions.

**[0041]** Fig. 5 is a flow diagram that provides an overview of methods used to execute a debit using the payment network 100 described above. A financial transaction between a merchant and a customer may be initiated by a customer selecting 500 a variety of purchase items or services. Purchase items may be selected 500 at a physical merchant site or a virtual site, such as an Internet site, provided by the merchant. After selecting the items, the customer then provides 502 a credential assigned to the customer to access the payment network 100 as payment for the items or services. In some cases, the credential may include

a PIN associated with the customer's payment network account. The customer may enter the PIN into a point-of-sale (POS) device or otherwise provide the PIN to the merchant.

**[0042]** When the merchant has access both to details of the transaction, and the credential, the merchant generates 504 an information packet. By way of example, this information packet may be generated by a POS device located at the merchant site, a computer system hosting a merchant Internet site, or other type of merchant processor. The information packet usually includes at least a specification of the amount of the transaction, an identification of the merchant, and the credential. The information packet may also include additional information.

**[0043]** The information packet is then transmitted 506 from the merchant to the transaction gateway 208. If the credential includes a PIN, the transaction gateway may verify the PIN provided is associated with the customer payment network account. If the correct PIN is not provided, the transaction gateway may transmit a authorization code to the merchant indicating denial of the financial transaction and the method may end. Otherwise, if the correct PIN is provided (or a PIN is not required to access the payment network account), the transaction gateway 208 uses the credential comprised by the information packet to determine 508 routing information for the payment network account. The routing information may be for one or more financial accounts maintained by the customer at one or more financial institutions that are associated with the credential. In embodiments in which more than one financial account is associated with the credential, the transaction gateway 208 may also determine how the cost of the financial transaction is to be allocated between the financial accounts. As previously described, the transaction gateway 208 may access instructions provided by the customer or may use a default algorithm (e.g., apportioning the costs equally among the identified financial accounts) to determine how the cost is allocated.

**[0044]** The routing information is transmitted 510 to the transaction system 220 with the other information from the information packet like merchant identification and transaction amount for the identified financial account(s). The routing information is used by the authorization module 224 of the transaction system to generate 512 an authorization packet for each of the financial account(s). The authorization packet includes the financial account, associated authorization information, and the amount of the transaction to be applied to the financial account.

[0045] In some embodiments, the merchant may have the option of having the transaction guaranteed by the payment network 100. There are a number of different arrangements by which requests for guaranteed transactions may be initiated. For example, in some embodiments, all authorizations may be treated as guaranteed or all authorizations may be treated as non-guaranteed. In other embodiments, a merchant processor may pass an indicator with the information packet that specifies on a transaction-by-transaction basis whether the transaction is to be treated as guaranteed or non-guaranteed. In still other embodiments, rules may be established for implementation by the authorization module to define when to treat transactions as guaranteed or non-guaranteed. Such rules may account for such factors as the size of the transaction, the nature of the goods and/or services being sold, the identity of the customer, and the like.

[0046] A determination 514 is thus made in accordance with these different criteria whether a transaction is to be treated as a guaranteed transaction. If so, the transaction system 220 performs 516 a risk analysis of the transaction to determine whether to provide the guarantee. Such a risk analysis may take account of a variety of factors, such as the size of the transaction, the credit history of the customer, and the like, and may use standard techniques known to those of skill in the art in evaluating the risk. If the risk level associated with the transaction is acceptable, then the transaction is executed as a guaranteed transaction; if the risk level is determined to be unacceptably high, the transaction may be declined or an option may be fed back through the transaction gateway 208 to offer the merchant the possibility of treating the transaction as a non-guaranteed transaction. This provides a mechanism for overriding the predetermined factors defining when to treat a transaction as guaranteed, and offers the merchant an opportunity to determine whether to accept the transaction as a non-guaranteed transaction.

[0047] The transaction system 220 seeks an authorization code for the transaction from the financial institution(s) that holds the account(s) to be debited. Seeking such an authorization code begins by transmitting 518 the authorization packet(s) that was generated 512 to the financial institution 140 associated with the financial account. Such transmittal may take place through any suitable debit-transaction mechanism, including the ACH system 120, the debit system 124, or a direct-to-bank connection to the financial institution 140 associated with the account.

**[0048]** In one embodiment, the transaction system 220 may select from a plurality of possible transaction networks that may be used to perform the debit transaction. By way of example, the transaction networks from which the transaction system 220 may select may include the ACH system 120, the debit system 130, or direct-to-bank connection. The processor may set up logical rules to determine which transaction network to select. For instance, the transaction network may be selected based on a risk analysis of the financial transaction performed by the processor. Higher risk transactions may be processed on a transaction network with higher transaction costs but with little or no risk that funds will be available to cover the costs. Similarly, lower risk transactions may be processed on a transaction network with lower transaction costs but having a higher risk that funds may not be available to cover the costs. By way of example, higher risk transactions may use the debit system 130, while lower transactions may use the ACH system 120. Other criteria, such as whether the merchant 110 requests a guarantee 514, may also be used to select the transaction network.

**[0049]** For each of the financial accounts for which an authorization packet was generated, the respective financial institution 140 at which the account is maintained determines 520 whether the account identified by the authorization packet has sufficient cleared funds to support the transaction and transmits 522 an authorization code back to the transaction system 220 to reflect its determination. If the account has sufficient cleared funds and there are no other derogatory marks associated with the account, the authorization code comprises an approval of the transaction, while a failure to meet those conditions results in the authorization code comprising a denial of the transaction.

**[0050]** The transaction system 220 may, in some embodiments, be equipped to perform additional operations related to the transaction. Merely by way of example, Fig. 5 note that in some embodiments, loyalty factors may be applied 524 to the transaction. Such loyalty factors typically require monitoring an accumulated transaction amount associated with an individual customer, perhaps based on certain defined classifications of transactions, so that rewards may be provided to the customer when certain accumulation levels are met. Such rewards may take the form of points that may be redeemed to purchase items from the merchant, for air travel or other products, or may take the form of cash rewards that are deposited directly to the customers identified account, and the like. Still other types of operations additional to coordination of the debit transaction will be known to those of skill

in the art and may be applied to transactions in other embodiments. In other embodiments, additional operations may not be performed.

**[0051]** The transaction system 220 transmits 526 the received authorization code(s) to the transaction gateway 208. In embodiments in which an authorization packet was  
5 generated 512 for only one financial account, the transaction gateway may then transmit 528 the authorization code to the merchant 110 in accordance with the authorization code received from the financial institution 140. In embodiments in which more than one financial account is used to pay for the financial transaction, the transaction gateway 208 may transmit 528 an authorization code to the merchant indicating approval of the transaction if all  
10 authorization code(s) received in response to the authorization packets indicated approval. Otherwise, if one or more authorization code(s) received by the transaction gateway 208 indicate denial of the transaction, the transaction gateway 208 may transmit 528 an authorization code to the merchant indicating denial of the transaction. The merchant makes a determination 530 whether to accept or decline the transaction based on the authorization  
15 code, usually acting in strict accordance with the recommended acceptance or rejection of the transaction transmitted 528 by the transaction gateway.

**[0052]** In an alternate embodiment, if a denial to one or more authorization code(s) received from a financial institution 140 indicates denial of the debit transaction, the transaction gateway 208 may attempt to debit the amount from an alternate account. Thus,  
20 the transaction gateway 208 may determine 508 routing information for a second financial account different than the denied account from which the apportionment of the cost allocated to the denied account may be debited. The then continue with 510 until an authorization code is received 522 for the second financial account. The second financial account may be determined by instructions associated with the customer credential or other default algorithm.  
25 If denial to the second account is received 522, the transaction gateway 208 may attempt to initiate a debit transaction for the denied amount from a different account associated with the credential or may transmit 528 an authorization code indicating denial of the transaction.

**[0053]** In some instances, because the way the transaction information is routed as described above, the returned code may be converted from one form to another by the  
30 transaction system 220 or transaction gateway 208. In particular, such conversion is typically performed so that the merchant 110 may make its decision whether to accept or decline the transaction based on the type of code response expected without substantial modification of

its system. For example, in an embodiment where the merchant is equipped to receive credit-based authorization codes and transmits the authentication packet in a form that requests execution of a guaranteed transaction, the code returned to the transaction gateway 208 may take the form of a debit-based authorization code. In such an embodiment, the transaction gateway 208 may convert the debit-based code to a corresponding credit-based code that is easily understood by existing merchant systems.

**[0054]** In some embodiments, reporting capabilities may be provided to the customers. These reports may allow a customer to view previous transactions for the customer that were paid for using the customer's credentials. Alternately or additionally, reports may also be provided to merchants to allow the merchant to view merchant transactions that used payment network 100.

**[0055]** In the foregoing description, for the purposes of illustration, methods were described in a particular order. It should be appreciated that in alternate embodiments, the methods may be performed in a different order than that described. It should also be appreciated that various modifications, alternative constructions, and equivalents may be used without departing from the spirit of the invention. Accordingly, the above description should not be taken as limiting the scope of the invention, which is defined in the following claims.